UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/364,835	07/30/1999	BAIJU V. PATEL	INTL-0182-US	9974

21906 7590 04/25/2006

TROP PRUNER & HU, PC
8554 KATY FREEWAY
SUITE 100
HOUSTON, TX 77024

EXAMINER	
HA, LEYNNA A	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/364,835
Filing Date: July 30, 1999
Appellant(s): PATEL ET AL.

Intel Corporation
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed January 26, 2006 appealing from the Office action mailed August 9, 2005

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is not all correct.

For independent claim 1, appellant discusses the IP security routine 411 which determines whether the security processing is to be offloaded. This feature is not recited in claim 1. The appellant also brief on a network controller 52 selecting a security service and process the data for encryption and authentication based the type or types of algorithms as indicated in the IPSEC packet. These features are not recited in claim 1.

For independent claim 13, appellants describes a driver security routine 410 which determines if a packet received has been "punted". This feature is not recited in claim 13.

For independent claim 28, appellant discusses the IP security routine 411, network controller 52, IPSEC packet, which are not recited in claim 28. It is reminded to the appellant that this section is summary of claimed subject matter not summary of appellant invention. Thus, claimed limitations are reasonably interpreted with the plain meaning in the art of computer security.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,546,463	Caputo, et al.	08-1996
5,268,962	Abadi, et al.	12-1993

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-5, 16-20, and 28-37 are rejected under 35 U.S.C. 102(b) as being anticipated by Caputo, et al. (US 5,546,463).

As per claim 1:

Caputo discloses a method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block; **[col.6, lines 18-21; security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the**

data packet during and/or after transmission of the data block. Caputo determines the verification process based on the algorithm chosen to implement.]

generating security information to pass along with the data block, the security information identifying the security service; and **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]**

using a computer peripheral device adapted to control communication with the communications channel **[see col.4, lines 24-44]** to select the security service from other security services based on the security information; and **[col.5, lines 48-67 and col.8, lines 59-67]**

processing, in a computer peripheral device, the data block according to the security information; **[see col.6, lines 22-35]**

As per claim 2: see col.6, lines 22-35; discusses performing cryptographic processing of the data block.

As per claim 3: see col. 8, lines 47-54; discusses receiving the data block from a software routine and routing the processed data block back to the software routine after processing.

As per claim 4: see col.6, lines 18-51; discloses determining if the security service can be performed by the computer peripheral device and if not,

processing the data block according to the security service in a software routine instead of the computer peripheral device **[see col.8, lines 47-54]**.

As per claim 5: see col.8, lines 11-16 and col.9, lines 21-22; discussing the Internet Protocol Security.

As per claim 16:

Caputo discusses a controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data **[see col.5, lines 11-15 and col.8, lines 10-16]** and associated security control information, the security control information **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]** identifying a security service to be performed on the data; and **[col.6, lines 18-21 and col.8, lines 11-16; security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo determines the verification process based on the algorithm chosen to implement.]**

a cryptographic engine **[see col.2, lines 20-63 and col.5, lines 17-24]** to select the security service from other security services based on the security control information **[col.5, lines 48-67]** and cryptographically processes the

data selection, the cryptographic engine being in the computer peripheral device. **[see col.6, lines 22-35 and col.8, lines 59-67]**

As per claim 17:

Caputo discusses the storage device containing information identifying security services to be performed **(see col.6, lines 18-21 and col.8, lines 11-16)**, the received security control information selecting a portion of the security services information in the storage device **(col.5, lines 48-67)**, wherein the cryptographic engine processes the data according to the selected portion of the security services information. **(see col.6, lines 22-35 and col.8, lines 59-67)**

As per claim 18: see col.5, lines 45-67 and col.7, lines 20-25; discussing a device adapted to change the contents of the storage device to update the security services information. **[it is inherent in the art that updating to make sure the system doesn't have outdated or unnecessary data and updating inherently helps the security of a system operate more efficiently.]**

As per claim 19: see col.5, lines 45-67 and col.8, lines 11-16; discussing a device adapted the security services information based on a predetermined replacement policy. **[it is inherent in the art that a replacement policy ensures the system doesn't have outdated or unnecessary data that would cause the system to slow down or takes longer period of time to process and because a replacement policy inherently further helps the security of a system.]**

As per claim 20: see col.6, lines 1-36 and col.8, lines 11-16; discussing the security services information includes security association information.

As per claim 28:

Caputo discloses a method for use in a device coupled to a communications channel, comprising:

determining a security service to perform with a data block; **[col.6, lines 18-21 and col.8, lines 11-16; security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo determines the verification process based on the algorithm chosen to implement.]**

generating security information to pass along with the data block **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]**, the security information identifying at least one of an encryption algorithm **[see col.5, lines 45-50]** and an authentication algorithm **[see col.6, lines 7-16]** to be performed by the security service; and **[see col.4, lines 30-44]**

processing, in a computer peripheral device adapted to control communication with the communications channel **[see col.4, lines 24-44]**, the data block according to the security information. **[see col.6, lines 18-35 and col.8, lines 59-67]**

As per claim 29: see col.5, lines 21-23; discusses the processing includes performing cryptographic processing of the data block.

As per claim 30: see col. 8, lines 47-54; discusses receiving the data block from a software routine and routing the processed data block back to the software routine after processing.

As per claim 31: see col.6, lines 18-51; discloses determining if the security service can be performed by the computer peripheral device and if not, processing the data block according to the security service in a software routine instead of the computer peripheral device. **[see col.8, lines 47-54]**

As per claim 32: see col.8, lines 11-16 and col.9, lines 21-22; discusses identifying a security service according to an Internet Protocol security protocol.

As per claim 33:

Caputo discloses a controller for controlling communications with a transport medium, the controller comprising:

a receiving circuit to receive data **[see col.5, lines 11-15 and col.8, lines 10-16]** and associated security control information **[see col.6, lines 1-18; the security information is the type of algorithm chosen for encryption/decryption or authentication algorithm to authenticate the data communicated and necessary for the recipient to verify in the verification process]**, the security control information identifying at least one of an encryption algorithm **[see col.5, lines 45-50]** and an authentication algorithm **[see col.6, lines 7-16]** to be performed on the data; and **[see col.4, lines 30-44]**

a cryptographic engine to cryptographically process the data based on the security control information **[see col.6, lines 18-35 and col.8, lines 59-67]**, the cryptographic engine being a computer peripheral device. **[col.5, lines 16-29]**

As per claim 34: see col.5, lines 19-20 and 48-50; discusses a storage device containing information identifying security services to be performed, the received security control information selecting a portion of the security services information in the storage device, wherein the cryptographic engine processes the data according to the selected portion of the security services information.

As per claim 35: see col.5, lines 45-67 and col.7, lines 20-25; discusses a device adapted to change the contents of the storage device to update the security services information. **[it is inherent in the art that updating to make sure the system doesn't have outdated or unnecessary data and updating inherently helps the security of a system and to operate more efficiently]**

As per claim 36: see col.5, lines 45-67 and col.8, lines 11-16; discusses the device is adapted to update the security services information based on a predetermined replacement policy. **[it is inherent in the art that a replacement policy to makes sure the system doesn't have outdated or unnecessary data that would cause the system to slow down or takes longer period of time to process and because a replacement policy inherently further helps the security of a system]**

As per claim 37: see col.5, lines 44-50 and col.6, lines 7-16 ; discusses the security services information includes security association information.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 13-15 are rejected under 35 U.S.C. 102(b) as being anticipated by Abadi, Et Al. (US 5,268,962).

As per claim 13:

Abadi discloses an article including a machine-readable storage medium containing instructions for execution in a system including a computer peripheral device adapted to control communication with a communications channel, the instructions when executed causing the system to: **(see FIG.3)**

receive a data block from the computer peripheral device; **(see col.5, lines 52-55)**

determine from information in the data block if a security service has not been performed on the data block by the computer peripheral device; and **[see col.3, lines 61-65 and col.4, lines 24-27; security service is the type of security**

rendered for the data packet prior to transmitting the packet to the host/destination. Abadi determines the security measure needed for the packet according to the other host by identifying the encryption key needed to encrypt the data packet and its destination so that the packet will transmit to the proper host that can decrypt the packet.]

process the data block if the security service has not been performed on the data block by the computer peripheral device. **[See col.4, lines 30-31 and col.6, lines 67-68; the network controller 116 is considered as the claimed computer peripheral device because it is a computer component connected to the host computer D via the DMA interface and cryptographic processing is the process of encryption or decryption.]**

As per claim 14: see col.7, line 63 - col.9, line 3; discussing the instructions causing the system to retrieve security information associated with the data block and sent the data block and security information to the computer peripheral device to perform the security service.

As per claim 15: see col.6, lines 7-63; discussing the instructions causing the system to perform the security service on the data block.

(10) Response to Argument

Claims 1-7, 16-20, and 28-37 is rejected over Caputo, et al.

Claim 1 states generating security information that is passed along with a data block, the security information identifying the security service. The security information can be interpreted as any data that identifies the type of service to ensure protection for a device, system, or a user, etc. This security data is reasonably information for a particular algorithm, password, or information of a user to identify the user wherein any of these information can be used to ensure the data block that and sent was not tampered with and that the data block is from a secure sender **[col.6, lines 1-12]**. Caputo does teach generating the security information that is pass along with the data block because it is necessary for the recipient to verify in the verification process. In addition, the data is transmitted in encrypted form whereby proper decryption is necessary to obtain the data. The decryption is necessary where the decryption algorithm obtain the data sent. Therefore, the encrypted data is the data what was once the plaintext data and now has a particular type of encryption involved which is the security service based on the security information being transmitted in the encrypted message **[col.5, lines 43-67]**. Caputo teaches the verification or authentication process that includes the generated security information passed along with the data block where the key is compared with encrypted item received and if there is a match, the user is

properly authenticated. Further, Caputo discusses digital signatures are also a form of authentication where the signer has a unique private key and the verification process uses a companion public key to verify if the signature is valid **[col.6, lines 39-67 and col.7, lines 15-20]**. Caputo teaches security information contained with the data block or in the message where this information is the type of algorithm that may contain a key chosen for encryption/decryption of the data in the data block or a digital signature for authentication to authenticate the data (message) transmitted **[see col.7, lines 30-60]**. Caputo disclose the security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo is able to select a security service by choosing from a variety of cryptographic algorithms **[col.5, lines 45-50]** and determines the authentication process based on the authentication algorithm chosen **[col.6, lines 8-26]**.

Claim 16 states a receiving circuit to receive data and associated security control information, the security control information identifying a security service to be performed on the data. Caputo discloses the encrypted block is sent to the challenger which is the receiver that compares and verifies the received data where the analogue and/or digital circuitry is used **[col.7, lines 15-19 and 55-60]** at the communication interface in the form of receiving circuit **[col.9, lines 15-16]**. Caputo discloses that the modem, encryptor, and

communication port responds to control signals to provide cryptographic functions **[col.5, lines 20-26]**. The cryptographic engine is the modem which is a computer peripheral device where encrypted block is passed to the modem where the encrypted data will be decrypted **[col.9, lines 118-22].** Caputo disclose the security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo is able to select a security service by choosing from a variety of cryptographic algorithms **[col.5, lines 45-50]** and determine the verification process based on the algorithm chosen to implement **[col.6, lines 18-21].**

Claim 28 states generating security information that is passed along with a data block, the security information identifies the encryption and authentication algorithm. This security data may be information for a particular algorithm, password, or information of a user to identify the user wherein any of these information can be used to ensure the data block that was sent was not tampered with and that the data block is from a secure sender **[col.6, lines 1-12]**. Caputo teaches the verification or authentication process that includes the generated security information passed along with the data block where the key is compared with encrypted item received and if there is a match, the user is properly authenticated. Further, Caputo discusses digital signatures are also a form of authentication where the signer has a

unique private key and the verification process uses a companion public key to verify if the signature is valid **[col.6, lines 39-67 and col.7, lines 15-20]**. Caputo teaches security information contained with the data block or in the message where this information is the type of algorithm that may contain a key chosen for encryption/decryption of the data in the data block **[see col.6, lines 1-20]**. In addition, the data is transmitted in encrypted form whereby proper decryption is necessary to obtain the data wherein the encrypted data is the data what was once the plaintext data and now has a particular type of encryption involved which is the security service based on the security information being transmitted in the encrypted message **[col.5, lines 43-67]**. Caputo discloses the security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo is able to select a security service by choosing from a variety of cryptographic algorithms **[col.5, lines 45-50]** and determine the authentication process based on the authentication algorithm chosen **[col.6, lines 8-26]**.

Claim 33 states a receiving circuit to receive data and associated security control information, the security control information identifying at least one of an encryption algorithm and an authentication algorithm to be performed on the data. Caputo discloses the encrypted block is sent to the challenger which is the receiver that compares and verifies the received data where the analogue

and/or digital circuitry is used **[col.7, lines 15-19 and 55-60]** at the communication interface in the form of receiving circuit **[col.9, lines 15-16].** Caputo discloses that the modem, encryptor, and communication port responds to control signals to provide cryptographic functions **[col.5, lines 20-26]**. The cryptographic engine is the modem which is a computer peripheral device where encrypted block is passed to the modem where the encrypted data will be decrypted **[col.9, lines 118-22].** Caputo disclose the security service is the type of security such as the type of encryption/decryption, authentication or verification process rendered for the data packet during and/or after transmission of the data block. Caputo is able to select a security service by choosing from a variety of cryptographic algorithms **[col.5, lines 45-50]** and determine the authentication process based on the authentication algorithm chosen **[col.6, lines 8-26].**

Dependent claims 2-12, 17-20, 29-32, 34-37 are rejected for at least the reason that these claims depend from.

Claims 13-15 remains rejected over Abadi.

As for claim 13, Abadi teaches a buffer queue index value (BQI) that specifies which of the buffer queues in the destination host computer the data packet should be sent to **[col.1, lines 43-46]**. The BQI and host-to-host key are included in the packet header where the packet is transmitted to another host computer where the key value is need to computer a decryption key

[col.4, line 50-col.5, line 5]. It is necessary for one computer to transmit or communicate data packets and processing the received data packets at another computer involves instructions where the instructions does the processing and determination as part of the computer system. According to such instructions, Abadi teaches the advantage of including the encrypted key value in the transmitted data packet is the receiving network controller able to compute the key value needed to decrypt the received data packet, hence, are instructions to determine and process the security service such as the proper decryption method to obtain the encrypted data packet **[col.1, lines 32-48 and col.5, lines 1-6]**. Further, Abadi discusses the packet header stores KeyIndex value that identifies which slot in the other host computer's Key Table holds the key needed to decrypt the data packet **[col.8, lines 61-66]**. Appellant's broadly claims security service where this limitation can reasonably be as any type of service that relies on security prevention methods and safeguards the user or the computer system. The security services of Abadi regards to encryption and having the proper decryption to obtain the encrypted packet received and having the values that identifies which slot the key for decryption **[col.9, lines 17-30]**. Therefore as discussed above, Abadi does teach instructions that perform the determination and processing of the security services involved in the data block.

Abadi's invention includes programs that causes instructions to be executed when Host A transmits data packet that contains instructions of the

security service involved for the data to be transmitted to the Host D where the packet contains information (i.e. source identification data, data packet value, encryption key, BQI value, slot identification) of the security service **[col.1, lines 32-48 and col.9, lines 17-30]**. For one computer to transmit or communicate data packets and processing the received data packets at another computer involves instructions where the instructions does the processing and determination. Hence, these instructions are executed for Host A to select the BQI value based on the user in Host D **[col.5, lines 18-22]** to verify the BQI value in a particular packet if a security service has been performed by comparing to the record if there is a match and if the BQI value is invalid **[see col.6, lines 8-23]**. Being invalid determines the security services was not allocated, thus was not performed because the invalid BQI cannot determine the decryption key that would execute the decryption service. Once compared and matched to the record, BQI value then leads to generating a decryption key for decrypting the encrypted portion of the received packet **[see col.6, lines 25-36]**. The BQI value is the information that determines whether a security service was performed by reading the header of each of the received data packet in order to process the BQI value and to generate the decryption key **[see col.5, lines 57-60 and col.6, lines 25-26]**. Abadi determines whether to discard or handle the data packets invalid BQI values **[see col.6, lines 22-23]**. The BQI has to be determined in order to know where to transfer to the buffer queues and generates a decryption key. Hence, if the BQI is not determined,

then the packet does not contain the security service needed to transfer to the Host D and thus, is not able to determine the buffer queue. Abadi shows that the determination of having security service is when the host-to-host key and the BQI is present for data transmission and if not present, any two host computers must first agree on the host-to-host encryption key **[col.3, lines 60-65]**.

As per claim 14, the examiner traverses appellant's argument that Aabadi fails to teach instructions that cause a system to retrieve security information associated with a data block and send the data block and security information to a computer peripheral device to perform security service because as discussed above, with instructions being necessary is part of any computer system to execute and perform determining functions and processing functions for data communication from one computer to another. Abadi invention includes programs that causes instructions to be executed when Host A transmits data packet that contains instructions of the security service involved for the data to be transmitted to the Host D where the packet contains information (i.e. source identification data, data packet value, encryption key, BQI value, slot identification) of the security service **[col.1, lines 32-48 and col.9, lines 17-30]**. According to such instructions, Abadi teaches the advantage of including the encrypted key value in the transmitted data packet is the receiving network controller able to compute the key value needed to decrypt the received data packet, hence, are instructions to determine and

process the security service such as the proper decryption method to obtain the encrypted data packet **[col.1, lines 32-48 and col.5, lines 1-6]**. Further, Abadi discusses the packet header stores KeyIndex value that identifies which slot in the other host computer's Key Table holds the key needed to decrypt the data packet **[col.8, lines 61-66]**. In addition, Adabi discloses instructions that causes a system to retrieve information where before exchanging data packets with any other host computer, the host computer must first establish a host-to host key and once the host-to-host key is established, each host uses its network controller to encrypt that key with its master key wherein generating values and stored in a Key Table **[col.4, lines 25-44]**. The host-to-host key must first be established leads to point out that the security service must be determined where the host-to-host key and the BQI is necessary to transmit secure data packets **[col.4, lines 48-67].**

For the explanations above, the examiner requests the Board not reverse the rejection.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

Leynna Ha LH

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Kim Vu – SPE KV

Hosuk Song – PE HS

TIMOTHY N TROP

TROP, PRUNER, & HU, P.C.

8554 KATY FREEWAY

SUITE 100

HOUSTON, TX 77024